Chapter 3

Invariants for multiple qubits: the case of 3 qubits

David A. Meyer* and Noland Wallach

Abstract The problem of quantifying entanglement in multiparticle quantum systems can be addressed using techniques from the invariant theory of Lie groups. We briefly review this theory, and then develop these techniques for application to entanglement of multiple qubits.

3.1 Introduction

In quantum mechanics the state of a closed system is most completely described by a unit vector in a complex Hilbert space. (Such a state is *pure* in physics terminology.) For many systems, e.g., those characterizable as consisting of multiple particles, the Hilbert space has a natural decomposition into tensor factors. The standard model of quantum computation presumes an ability to implement unitary transformations which decompose into polynomially (in the number of factors, each of

*This work was supported in part by the National Security Agency (NSA) and Advanced Research and Development Activity (ARDA) under Army Research Office (ARO) contracts DAAG55-98-1-0376 and DAAD19-01-1-0520.

1-58488-282/4/02/$0.00+$1.50

which is of no more than some constant dimension) many unitary transformations acting nontrivially on only one or two factors [1]. Such a decomposition of states and operations makes possible the exponential reduction in complexity of, for example, the quantum Fourier transform relative to even the fast classical Fourier transform [2,3], and suggests, more generally, that quantum computation may be more powerful than classical computation.

It has been recognized, of course, since the famous paper of Einstein, Podolsky and Rosen [4], that the quantum description of a multiparticle system differs greatly from any classical description which decomposes in the same way. Bohm distilled their two particle example to its essence by considering pairs of spin-$\frac{1}{2}$ particles, i.e., systems described by elements of the Hilbert space $\mathbb{C}^2 \otimes \mathbb{C}^2$ [5]. For this example, Bell's Theorem specifies exactly the limits of any classical description [6]; these limits are maximally exceeded by the "singlet" state $(|01\rangle - |10\rangle)/\sqrt{2}$. (Here, and subsequently, we use Dirac notation $|\cdot\rangle$ to denote elements of Hilbert space, $\langle\cdot|$ for dual elements, use $|0\rangle$ and $|1\rangle$ as a basis for $\mathbb{C}^2$, and write $|01\rangle = |0\rangle \otimes |1\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$.) In fact, they are exceeded equally by any state obtained from the singlet state by unitary transformations which decompose in the same way as the Hilbert space, i.e., elements of $U(2) \times U(2)$. According to the terminology introduced by Schrödinger [7], these states are equally *entangled*.

More precisely, an element of a Hilbert space with a specified tensor product decomposition, $V = V_1 \otimes \cdots \otimes V_n$, is *not entangled* if and only if it can be written as a product $v_1 \otimes \cdots \otimes v_n$ with $v_i \in V_i$. A *measure of entanglement* is a function $f : V = V_1 \otimes \cdots \otimes V_n \to \mathbb{C}$ that is invariant under $U(V_1) \times \cdots \times U(V_n)$.

In keeping with our interest in quantum computation (and because they are easiest), in this paper we will consider only cases when each of the tensor factors is two dimensional, i.e., a qubit. The situation considered by Bohm [5], for example, is a pair of qubits. From a general state $v \in \mathbb{C}^2 \otimes \mathbb{C}^2$, familiar constructions in physics are the *density matrix*

$$\rho = v \otimes v^* \in (\mathbb{C}^2 \otimes \mathbb{C}^2) \otimes (\mathbb{C}^2 \otimes \mathbb{C}^2)^*,$$

and the *reduced density matrix* $\tilde{\rho} = \mathrm{Tr}_2\rho$. In a basis, $\rho = \sum \rho_{ijkl}|ij\rangle\langle kl|$ and $\tilde{\rho} = \sum \rho_{ijkj}|i\rangle\langle k|$. Notice that the cyclic property of trace implies that $\tilde{\rho}$ is invariant under $I \times U(2)$. The usual analysis continues by observing that the eigenvalues λ_i of $\tilde{\rho}$ are therefore invariant under $U(2) \times U(2)$, and constructing the *entropy*, $-\sum \lambda_i \log \lambda_i$, to quantify the entanglement of the bipartite state v from which ρ and $\tilde{\rho}$ were constructed. The eigenvalues of $\tilde{\rho}$ are the solutions of the characteristic equation $0 = \lambda^2 - (\mathrm{Tr}\tilde{\rho})\lambda + \det\tilde{\rho}$; the functions $\mathrm{Tr}\tilde{\rho} = 1$ and $\det\tilde{\rho}$ contain the same information as the eigenvalues. These functions are, in fact, invariants of $U(2) \times U(2)$, which are *polynomials* in the coefficients of $v = \sum v_{ij}|ij\rangle$ and $v^* = \sum\langle ij|\bar{v}_{ij}$; explicitly, $\det\tilde{\rho} = \det[v_{ij}]\det[\bar{v}_{ij}]$.

As others have noted [8–12], identifying such measures of entanglement is thus a problem in the invariant theory of Lie groups. In Section 3.2 we provide a brief introduction to the techniques of this theory, emphasizing the role of polynomial invariants. It is relatively straightforward to apply these techniques to small numbers of qubits; we do so for 1 and 2 qubits in Section 3.3, reproducing the result of the computation in the previous paragraph. Until recently, there was little understanding of entanglement for more than two factors, but this approach applies in principle to any number of factors. In Sections 3.4 and 3.5 we analyze the case of 3 qubits, obtaining a particularly nice set of generators and relations for the ring of invariants. These results are equivalent to, although in a different form and derived differently than the results of Grassl, Rötteler and Beth [10,13]. In particular, our approach has implications for entanglement invariants of 4 qubits; we sketch these in Section 3.6.

3.2 Invariants for compact Lie groups

Let W be a k dimensional vector space over K (the real numbers, $\mathbb{R}$, or the complex numbers, $\mathbb{C}$). Then a mapping $f : W \to \mathbb{C}$ is said to be a *polynomial* function if there exists a polynomial, φ, over $\mathbb{C}$ in variables $x_1, \ldots, x_k$ such that $f(\sum x_i w_i) = \varphi(x_1, \ldots, x_k)$. We will use the notation $\mathcal{P}(W)$ for the algebra of polynomials on W. We will also write $\mathcal{P}^d(W)$ for the space of polynomials of degree d. If V is a vector space over $\mathbb{C}$ but we are looking at V as a vector space over $\mathbb{R}$ then we will use the notation $\mathcal{P}_{\mathbf{R}}(V)$ and $\mathcal{P}^d_{\mathbf{R}}(V)$. Let G be a compact Lie group and let (π, V) be a finite dimensional unitary representation of G with V an n-dimensional complex Hilbert space. A function $f : V \to \mathbb{C}$ is said to be a *polynomial G-invariant* if $f(\pi(g)v) = f(v)$ for all $g \in G$ and $v \in V$ and $f \in \mathcal{P}_{\mathbf{R}}(V)$. We will write $\mathcal{P}_{\mathbf{R}}(V)^G$ for the G-invariant polynomials and $\mathcal{P}^d_{\mathbf{R}}(V)^G$ for the ones of degree d. The key reason for considering this class of invariants is that it is essentially the smallest

algebra that separates the orbits.

THEOREM 3.1

If $v, w \in V$ then $f(v) = f(w)$ for all $f \in \mathcal{P}_{\mathbb{R}}(V)^G$ if and only if there exists $g \in G$ such that $\pi(g)v = w$.

PROOF The function $v \mapsto |v|^2$ is an element of $\mathcal{P}_{\mathbb{R}}(V)^G$. Thus we may replace V by its unit sphere, $S(V)$, without any loss of generality. Since $S(V)$ is compact the Stone–Weierstrauss theorem implies that $\mathcal{P}_{\mathbb{R}}(V)$ is dense in the space of continuous functions on $S(V)$ in the uniform topology. Suppose that $\pi(G)v \cap \pi(G)w = \emptyset$. Urysohn's theorem implies that since $\pi(G)v$ and $\pi(G)w$ are compact there exists a real valued continuous function f on V such that $f(\pi(G)v) = \{1\}$ and $f(\pi(G)w) = \{0\}$. Let $\mathrm{d}g$ denote invariant measure on $\pi(G)$ normalized so that $\int_G \mathrm{d}g = 1$. If g is a continuous function on V define $f^\#(z) = \int_G f(\pi(g)z)\mathrm{d}g$. Then $f^\#(\pi(G)v) = \{1\}$ and $f^\#(\pi(G)w) = \{0\}$. Let $\phi \in \mathcal{P}_{\mathbb{R}}(V)$ be real valued and such that $|f^\#(z) - \phi(z)| < \frac{1}{4}$ for $z \in S(V)$. Then

$$
\begin{aligned}
\left|f^\#(v) - \int_G \phi(\pi(g)v)\mathrm{d}g\right| &= \left|\int_G (f^\#(v) - \phi(\pi(g)v))\mathrm{d}g\right| \\
&= \left|\int_G (f^\#(\pi(g)v) - \phi(\pi(g)v))\mathrm{d}g\right| \\
&\le \int_G |f^\#(\pi(g)v) - \phi(\pi(g)v)|\mathrm{d}g \\
&\le \frac{1}{4}.
\end{aligned}
$$

Thus $\phi^\#(\pi(g)v) \ge \frac{3}{4}$ and $\phi^\#(\pi(g)w) \le \frac{1}{4}$ for all $g \in G$. This implies the result. ∎

If we had used complex polynomials the analogous result would have been in general false.

We will set $\mathcal{P}(V)^G$ equal to $\mathcal{P}_{\mathbb{R}}(V)^G \cap \mathcal{P}(V)$. Let $\overline{V}$ denote V with the opposite complex structure. In other words we replace our choice, i, for $\sqrt{-1}$ by $-i$. If f is a function on V then we set $gf(x) = f(\pi(g)^{-1}x)$ for $g \in G$ and $x \in V$.

PROPOSITION 3.1

As a representation of G, $\mathcal{P}^d_{\mathbb{R}}(V)$ is equivalent with $\bigoplus_{0\le k\le d} \mathcal{P}^{d-k}(V) \otimes \mathcal{P}^k(\overline{V})$.

PROOF Let $v_1, \ldots, v_n$ be a basis of V. Then a vector in V can be written as $\sum z_i v_i$ with $z_i \in \mathbb{C}$. Hence an element of $\mathcal{P}^d_{\mathbb{R}}(V)$ can be written as a polynomial of degree d in $z_1, \ldots, z_n, \overline{z}_1, \ldots, \overline{z}_n$. Such a polynomial is written as a sum of products of polynomials of degree $d-k$ in $z_1, \ldots, z_n$ and degree k in $\overline{z}_1, \ldots, \overline{z}_n$ for $0 \le k \le d$. The result now follows since the action of G on $\mathcal{P}^k(\overline{V})$ is equivalent to the action of G on $\overline{\mathcal{P}^k(V)}$ obtained by restricting the action of G on $\mathcal{P}^d_{\mathbb{R}}(V)$. ∎

Let $\widehat{G}$ denote the set of equivalence classes of irreducible (necessarily finite dimensional) unitary representations of G (here a representation is always assumed to be strongly continuous). If (σ, W) is a finite dimensional unitary representation of G then W splits into a direct sum of irreducible subrepresentations. If $\gamma \in \widehat{G}$ then we denote by $W(\gamma)$ the sum of all irreducible invariant subspaces of W that are in the class of γ. Then $\dim W(\gamma) = m_W(\gamma)d(\gamma)$, where $d(\gamma)$ is the dimension of any member of γ and $m_W(\gamma)$ is the multiplicity of γ in W. If $\gamma \in \widehat{G}$ then we denote by $\overline{\gamma}$ the class of a representation of G that is dual (or complex conjugate) to an element of γ. If $W = \mathcal{P}^k(V)$ as above then we set $m_{\mathcal{P}^k(V)}(\gamma) = m_{V,k}(\gamma) = m_k(\gamma)$ (if V is understood). Then clearly, $m_{\overline{V},k}(\overline{\gamma}) = m_{V,k}(\gamma)$.

The formal power series $h_V(q,t) = \sum_{i,j} q^i t^j \dim\left(\mathcal{P}^i(V) \otimes \mathcal{P}^j(\overline{V})\right)^G$ is called the bigraded Hilbert series of the polynomial invariants. Also, $h_V(q,q)$ is the usual Hilbert series of the polynomial G-invariants in V.

PROPOSITION 3.2

We have

$$h_V(q,t) = \sum_{i,j} q^i t^j m_i(\gamma) m_j(\gamma).$$

PROOF We note that $\left(\mathcal{P}^i(V)(\gamma) \otimes \mathcal{P}^j(\overline{V})(\tau)\right)^G$ is zero if $\gamma \ne \overline{\tau}$ and has dimension $m_i(\gamma)m_j(\gamma)$ if $\gamma = \overline{\tau}$. This implies the result. ∎

The above result indicates that we should define the q-multiplicity of

γ in $\mathcal{P}(V)$ to be the formal power series $m(q,\gamma) = \sum_j q^j m_j(\gamma)$. Then we have:

LEMMA 3.1
With the notation above,

$$h(q,t) = \sum_{\gamma \in \widehat{G}} m(q,\gamma) m(t,\gamma).$$

In the next sections we will describe the implications of these results to qubits, i.e., the case when $V = \bigotimes^k \mathbb{C}^2$ and G is a product of k copies of $K = SU(2)$ (or $U(2)$) acting by, e.g., $(g_1, g_2, g_3)(v_1 \otimes v_2 \otimes v_3) = g_1 v_1 \otimes g_2 v_2 \otimes g_3 v_3$. Note that product (i.e., unentangled) states form a single orbit of the group G. This indicates (in light of Theorem 3.1) that the G-invariant polynomials on $\bigotimes^k \mathbb{C}^2$ are measures of entanglement.

If $K = SU(2)$ then the irreducible unitary representations are parameterized by their spin, which is a nonnegative half integer, s; that is, $\widehat{K}$ is $\{s \in \mathbb{Z}/2 \mid s \geq 0\} = (\mathbb{Z}/2)_{\geq 0}$. We fix an element in the class of s, F^s and observe that $\dim F^s = 2s+1$. We choose $F^{\frac{1}{2}} = \mathbb{C}^2$. The corresponding parameterization of the irreducible unitary representations of G is $\left((\mathbb{Z}/2)_{\geq 0}\right)^k = \{(s_1, \ldots, s_k) \mid s_i \in (\mathbb{Z}/2)_{\geq 0}\}$. We choose $F^{\mathbf{s}} = F^{s_1} \otimes \cdots \otimes F^{s_k}$ as a representative of $\mathbf{s} = (s_1, \ldots, s_k)$.

3.3 The simplest cases

Before we get to more serious undertakings we will demonstrate our technique in the easiest cases.

Example 3.1
$k = 1$. Then we may take $F^s = \mathcal{P}^{2s}(\mathbb{C}^2)$. Thus $m_k(s) = \delta_{2k,s}$. This implies that

$$h_{\mathbb{C}^2}(q,t) = \sum_j (qt)^j = \frac{1}{1-qt}.$$

From this we see (the well-known fact) that all of the polynomial invariants of the action of $SU(2)$ on $\mathbb{C}^2$ are polynomials in $v \mapsto |v|^2$. $\square$

Example 3.2
$k = 2$. In this case one has

$$\mathcal{P}^k(\mathbb{C}^2 \otimes \mathbb{C}^2) = F^{(\frac{k}{2},\frac{k}{2})} \oplus F^{(\frac{k}{2}-1,\frac{k}{2}-1)} \oplus \cdots \oplus \begin{cases} F^{(0,0)} & \text{if } k \text{ is even} \\ F^{(\frac{1}{2},\frac{1}{2})} & \text{otherwise} \end{cases}.$$

From this we see that

$$m(q, (\frac{k}{2}, \frac{k}{2})) = \sum_{j \geq 0} q^{k+2j} = \frac{q^k}{1-q^2}.$$

This yields

$$\begin{aligned} h(q,t) &= \sum_k m(q, (\frac{k}{2}, \frac{k}{2})) m(t, (\frac{k}{2}, \frac{k}{2})) \\ &= \sum_k \frac{q^k t^k}{(1-q^2)(1-t^2)} \\ &= \frac{1}{(1-q^2)(1-qt)(1-t^2)}. \end{aligned}$$

This immediately imples that the invariants of the action of $SU(2) \times SU(2)$ on $\mathbb{C}^2 \otimes \mathbb{C}^2$ are polynomials in three invariants. The invariant corresponding to tq is $v \mapsto |v|^2$ and there is a "new" invariant defined as follows: if $v = \sum v_{ij} |ij\rangle$ then $f(v) = \det [v_{ij}]$. Notice that this is an element of $\mathcal{P}(\mathbb{C}^2 \otimes \mathbb{C}^2)^G$ (and in fact generates the algebra). The invariant f corresponds to q^2 and the complex conjugate of f corresponds to t^2. $\square$

In the above example we note that we could also have looked at the action of $U(2) \times U(2)$ on $\mathbb{C}^2 \otimes \mathbb{C}^2$. This is the same as the action of $S^1 \times G$ on $\mathbb{C}^2 \otimes \mathbb{C}^2$ via $(z,u,v)(x \otimes y) = z(ux \otimes vy)$. We note that $f(zv) = z^2 f(v)$. Thus the polynomial invariants of the action of $S^1 \times G$ are polynomials in $|v|^2$ and $|f(v)|^2$. These are exactly the invariants we described in the Introduction, namely $\mathrm{Tr}\tilde{\rho} = 1$ and $\det \tilde{\rho}$, respectively.

Although these examples are very simple, they illustrate an interesting feature of all such examples which will be useful subsequently. The representation $V = \bigotimes^k \mathbb{C}^2$ is equivalent with its complex conjugate. We are thus looking at the diagonal action of G on $\bigotimes^k \mathbb{C}^2 \oplus \bigotimes^k \mathbb{C}^2$. This can be interpreted as the action of G on $(\bigotimes^k \mathbb{C}^2) \otimes \mathbb{C}^2$ via $g \otimes I$. There is therefore a full $GL(2,\mathbb{C})$ acting by $I \otimes g$ that commutes with the action of G. This implies that $\mathcal{P}_{\mathbb{R}}(V)^G$ is naturally a representation

space for $GL(2,\mathbb{C})$. The action of the Lie algebra of this group can be described in terms of polarization operators. Choose an orthonormal basis $\{v_i\}$ of V; let z_i be the corresponding linear coordinates; and set $x = \sum z_i \frac{\partial}{\partial \bar{z}_i}$, $y = \sum \bar{z}_i \frac{\partial}{\partial z_i}$ and $h = \sum z_i \frac{\partial}{\partial z_i} - \sum \bar{z}_i \frac{\partial}{\partial \bar{z}_i}$. Then $[x,y] = h$, $[h,x] = 2x$, $[h,y] = -2y$. In the case when $k = 2$ we note that the invariants are generated by f, yf, and $y^2 f$. The span of this space is the spin-1 representation of $SL(2,\mathbb{C})$. We also note that we may restrict this action to $SU(2)$ and thereby we have made a partial decomposition of the case of *3 qubits*. Indeed, we have (using the classical theory of spherical harmonics):

$$m_{\otimes^3\mathbb{C}^2}(q,(0,0,\frac{k}{2})) = \begin{cases} 0 & \text{if } k \text{ is odd;} \\ \frac{q^{2k}}{1-q^4} & \text{if } k \text{ is even.} \end{cases}$$

We will describe the full decomposition in the next section. Note that the above formula implies that the q-multiplicity of the trivial representation in the case of 3 qubits is $(1-q^4)^{-1}$. We will now give a formula for an invariant of degree 4 which of necessity must generate all complex analytic polynomials for 3 qubits. Let

$$\left(\sum v_{ij}|ij\rangle, \sum w_{kl}|kl\rangle\right) = \sum \epsilon_{ik}\epsilon_{jl} v_{ij} w_{kl}$$

with $\epsilon_{ik} = 0$ if $i = k$; 1 if $i < k$; and -1 if $i > k$. Then $(\cdot,\cdot)$ defines a complex bilinear symmetric form on $\mathbb{C}^2 \otimes \mathbb{C}^2$ that is invariant under the action of $SU(2) \times SU(2)$. If $v \in \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ then we write $v = v_0 \otimes |0\rangle + v_1 \otimes |1\rangle$. The desired invariant of degree 4 is given by

$$f(v) = \det\left[(v_i, v_j)\right].$$

For example, if $v = (|000\rangle + |111\rangle)/\sqrt{2}$ then $v_0 = |00\rangle/\sqrt{2}$ and $v_1 = |11\rangle/\sqrt{2}$ so $(v_0,v_0) = 0$, $(v_1,v_1) = 0$, and $(v_0,v_1) = \frac{1}{2}$. Hence

$$f(v) = \det\begin{bmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{bmatrix} = -\frac{1}{4}.$$

In particular, f is not the zero polynomial so

$$\mathcal{P}(\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2)^{SU(2)\times SU(2)\times SU(2)}$$

is the algebra of polynomials in f.

3.4 The case of 3 qubits

In this section we will study the invariant polynomials under the action of $G = SU(2) \times SU(2) \times SU(2)$ acting on $\bigotimes^3 \mathbb{C}^2$. This means that we should be studying the real analytic (not complex analytic) polynomials on $V = \bigotimes^3 \mathbb{C}^2$. We will look at two cases. The first is the invariant theory for G and the second is that for $S^1 \times G$ acting via

$$(t, u_1, u_2, u_3)(v_1 \otimes v_2 \otimes v_3) = t(u_1 v_1 \otimes u_2 v_2 \otimes u_3 v_3),$$

the obvious action of $U(2) \times U(2) \times U(2)$. Both are a consequence of the decomposition of the space of complex analytic polynomials on V. If $\varsigma = (a,b,c)$ with $a,b,c \in (\mathbb{Z}/2)_{\geq 0}$ then set $m(\varsigma) = 2\min\{a,b,c\}$ and $n(\varsigma) = 2(a+b+c) - 2m(\varsigma)$. We note that if we write $\varsigma = a(\frac{1}{2},\frac{1}{2},\frac{1}{2}) + (b_1,b_2,b_3)$ with $a, b_i \geq 0$ and $b_1 b_2 b_3 = 0$ then $m(\varsigma) = a$ and $n(\varsigma) = a + 2(b_1+b_2+b_3)$. The following decomposition of the complex analytic polynomials on V under the action of G is taken from [14].

THEOREM 3.2
The algebra of G-invariants in the complex analytic polynomials on V consists of the polynomials in the invariant f described at the end of Section 3.3. Let Y denote the variety of all $v \in V$ such that $f(v) = 0$ and let $A^n(Y)$ denote the restriction of the space of polynomials of degree n to Y. Then $A^n(Y)$ decomposes into the multiplicity free direct sum of the representations with highest weight ς satisfying the following conditions:

$$n - n(\varsigma) \equiv 0 \ mod\ 2 \quad \text{and} \quad m(\varsigma) \geq \frac{n - n(\varsigma)}{2} \geq 0.$$

This result has as an immediate corollary (notation as in the discussion at the beginning of this section):

COROLLARY 3.1
We have

$$m(q,\varsigma) = \frac{q^{n(\varsigma)}(1 + q^2 + \cdots + q^{2m(\varsigma)})}{1-q^4} = \frac{q^{a+2(b_1+b_2+b_3)}(1+q^2+\cdots+q^{2a})}{1-q^4}$$

$$= q^{2(b_1+b_2+b_3)} q^a \frac{1-q^{2a+2}}{(1-q^2)(1-q^4)}.$$

We are now ready to give the bigraded Hilbert series of the invariants in this case.

PROPOSITION 3.3
We have

$$h(q,t) = \frac{(1+(qt)^2)(1+(qt)^2+(qt)^4)}{(1-qt)(1-q^4)(1-q^3t)(1-q^2t^2)(1-qt^3)(1-t^4)(1-(qt)^3)}.$$

PROOF Lemma 3.1 and the material above imply that (in the sums below $b_1b_2b_3 = 0$ means that we allow all possibilities of $b_i \geq 0$ where at least one of the b_i is 0):

$$h(q,t) = \sum_{\zeta} m(q,\zeta)m(t,\zeta) = \frac{1}{(1-q^4)(1-t^4)}$$
$$\sum_{b_1b_2b_3=0} (qt)^{2(b_1+b_2+b_3)} \sum_{a\geq 0} (qt)^a \frac{1-q^{2a+2}}{1-q^2} \cdot \frac{1-t^{2a+2}}{1-t^2}.$$

We note that we have in the sense of formal sums

$$\sum_{b_1b_2b_3=0} x^{b_1+b_2+b_3} = \frac{1}{(1-x)^3} - \frac{x^3}{(1-x)^3} = \frac{1-x^3}{(1-x)^3}$$

and

$$\sum_{a\geq 0} (qt)^a \frac{1-q^{2a+2}}{1-q^2} \cdot \frac{1-t^{2a+2}}{1-t^2} = \frac{(1-q^2)(1-t^2)(1-(qt)^4)}{(1-(qt)^3)(1-q^3t)(1-q^2t^2)(1-qt^3)}.$$

If we make the obvious substitution the result follows. ∎

Before we do any analysis of this formula we will look at the ordinary Hilbert series of the polynomial invariants for the above action of $S^1 \times G$ (there is no extra information in the bigraded Hilbert series since it would be a series in qt).

PROPOSITION 3.4
The Hilbert series for the polynomial invariants for the action of $S^1 \times G$

on $\bigotimes^3 \mathbb{C}^2$ is

$$h(q) = \frac{1+q^{12}}{(1-q^2)(1-q^4)^3(1-q^6)(1-q^8)}.$$

PROOF In this case we have that if $m(q,\zeta)$ is as above for G and if

$$m(q,\zeta) = \sum_{n\geq 0} a_n(\zeta) q^n$$

then

$$h(q) = \sum_{n\geq 0} q^{2n} \sum_{\zeta} a_n(\zeta)^2.$$

The argument for this is somewhat complicated. We will make some observations that follow from our formula for $m(q,\zeta)$. Define the non-negative integers $a_{n,m}$ by

$$\frac{1-q^{m+1}}{(1-q)(1-q^2)} = \sum_{n\geq 0} a_{n,m} q^n.$$

If

$$w_m(q) = \sum_{n\geq 0} a_{n,m}^2 q^n$$

then if we set

$$g(q) = \frac{1-q^6}{(1-q^2)^3} \sum_{m\geq 0} q^m w_m(q^2),$$

we have $h(q) = g(q^2)$. This leaves the calculation of the series $w_m(q)$. The formula depends on the parity of m: if $k \geq 0$ then

$$w_{2k}(q) = \frac{1+2(q^2+\cdots+q^{2k})-(2k+1)q^{2k+1}}{(1-q)(1-q^2)}$$

and

$$w_{2k+1}(q) = \frac{1+2(q^2+\cdots+q^{2k})-(2k+1)q^{2k+2}}{(1-q)(1-q^2)}.$$

We write $b_m(q) = (1-q^2)(1-q^4)w_m(q^2)$. Then

$$g(q) = \frac{1-q^6}{(1-q^4)(1-q^2)^4} \sum_{m\geq 0} q^m b_m(q).$$

Now

$$\sum_{m\geq 0} q^m b_m(q) = \sum_{k\geq 0} q^{2k}(1+2(q^4+\cdots+q^{4k})-(2k+1)q^{4k+2}) + \sum_{k\geq 0} q^{2k+1}(1+2(q^4+\cdots+q^{4k})-(2k+1)q^{4k+4}).$$

This expression can be written

$$\begin{aligned}
&\frac{1}{1-q}+2(1+q)\sum_{k\geq 0} q^{2k}(q^4+\cdots+q^{4k})-(1+q^3)q^2\sum_{k\geq 0}(2k+1)q^{6k}\\
&=\frac{1}{1-q}+2(1+q)q^4\sum_{k\geq 0} q^{2k}\frac{1-q^{4k}}{1-q^4}+\frac{(1+q^3)q^2}{1-q^6}-\frac{2(1+q^3)q^2}{(1-q^6)^2}\\
&=\frac{1}{1-q}+\frac{2(1+q)q^4}{(1-q^2)(1-q^4)}-\frac{2(1+q)q^4}{(1-q^4)(1-q^6)}\\
&+\frac{(1+q^3)q^2}{1-q^6}-\frac{2(1+q^3)q^2}{(1-q^6)^2}\\
&=\frac{(1+q^6)(1+q)}{(1-q^6)(1-q^3)}.
\end{aligned}$$

We therefore have

$$g(q)=\frac{1+q^6}{(1-q)(1-q^2)^3(1-q^3)(1-q^4)}.$$

Hence

$$h(q)=g(q^2)=\frac{1+q^{12}}{(1-q^2)(1-q^4)^3(1-q^6)(1-q^8)}.$$

∎

Our next task is to write out a basic set of invariants. This will be done in the next section.

3.5 A basic set of invariants for 3 qubits

In this section we construct a set of invariants for the action of $G = SU(2)\times SU(2)\times SU(2)$ on $V=\mathbb{C}^2\otimes\mathbb{C}^2\otimes\mathbb{C}^2$. We will first do this abstractly and then give more concrete formulae for the invariants which are necessary for our proof that they are, in fact, basic. We define an inner product $\langle\cdot,\cdot\rangle$ on $S(V)$ (the symmetric algebra on V) which is the restriction of the usual inner product on the tensor algebra:

$$\langle v_1\otimes\cdots\otimes v_k|w_1\otimes\cdots\otimes w_l\rangle=\langle v_1|w_1\rangle\cdots\langle v_k|w_k\rangle\,\delta_{k,l}.$$

As usual we will write $v^k=v_1\otimes\cdots\otimes v_k$ with $v_i=v$ for all $1\leq i\leq k$. Then $S(V)$ is the span of the v^k for $v\in V$ and $k\in\mathbb{Z}_{\geq 0}$. We will write $S^k(V)$ for the span of the elements v^k with $v\in V$. Since the representation of G on V is self dual the results we described for the decomposition of the (complex analytic) polynomial functions on V also describe the decomposition of $S(V)$. Thus we have that as representations of G:

$$\begin{aligned}
S^1(V)&=V=F^{(\frac12,\frac12,\frac12)}\\
S^2(V)&=F^{(1,0,0)}\oplus F^{(0,1,0)}\oplus F^{(0,0,1)}\oplus F^{(1,1,1)}\\
S^3(V)&=F^{(\frac12,\frac12,\frac12)}\oplus F^{(\frac12,\frac12,\frac32)}\oplus F^{(\frac12,\frac32,\frac12)}\oplus F^{(\frac32,\frac12,\frac12)}\oplus F^{(\frac32,\frac32,\frac32)}\\
S^4(V)&=F^{(0,0,0)}\oplus F^{(2,0,0)}\oplus F^{(0,2,0)}\oplus F^{(0,0,2)}\oplus F^{(1,1,0)}\oplus F^{(1,0,1)}\\
&\quad\oplus F^{(0,1,1)}\oplus F^{(1,1,1)}\oplus F^{(1,1,2)}\oplus F^{(1,2,1)}\oplus F^{(2,1,1)}\oplus F^{(2,2,2)}.
\end{aligned}$$

The bigraded formula above implies that there is one invariant of bidegree $(1,1)$, four linearly independent invariants of bidegree $(2,2)$, and one each of bidegrees $(4,0)$, $(3,1)$, $(1,3)$ and $(0,4)$. In bidegree $(3,3)$ there is a 1-dimensional space of invariants that cannot be a subspace of the algebra generated by the ones of lower degree. We assert that the nine dimensional space of invariants obtained from these observations generates the algebra of invariants. We will now give our first description of the desired invariants. Let P_ζ denote the projection onto the F^ζ constituents in each of the symmetric powers described above. Then there is only one $(1,1)$ invariant up to a scalar multiple and that must be $|v|^2$. In bidegree $(2,2)$ the following invariants span: $|v|^4$ and $\langle P_\zeta(v^2),v^2\rangle$ for $\zeta\in\{(1,0,0),(0,1,0),(0,0,1),(1,1,1)\}$. It is clear that $\sum_\zeta\langle P_\zeta(v^2),v^2\rangle=|v|^4$. Thus we can choose $\psi_j(v)=\langle P_{\varepsilon_j}(v^2),v^2\rangle$ with $\varepsilon_1=(1,0,0)$, $\varepsilon_2=(0,1,0)$ and $\varepsilon_3=(0,0,1)$. Up to a scalar multiple the only invariant of bidegree $(3,1)$ is obtained as follows. The above decomposition of $S^3(V)$ implies that there exists a unique (up to a scalar multiple) intertwining operator

$$T:V\to S^3(V)$$

(that is, $T(gv)=gT(v)$ for $g\in G$). We set $\psi_4(v)=\langle v^3,T(v)\rangle$ and $\psi_5(v)=\langle T(v),v^3\rangle$. It is clear that up to a scalar multiple the only

$(4,0)$ invariant is our original one, f, and the one of bidegree $(0,4)$ is its complex conjugate. Finally we set $\psi_6(v) = \langle P_{(\frac{1}{2},\frac{1}{2},\frac{1}{2})}(v^3), v^3\rangle$.

Our next task is to give more concrete descriptions of ψ_j, $1 \le j \le 6$. For this we must use a bit more of the structure of the representation of G on $V = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$. We observe that there is a symplectic structure over $\mathbb{C}$. Indeed, if we write

$$\begin{aligned} v &= v(x,y) \\ &= x_1|000\rangle + x_2|011\rangle + x_3|101\rangle + x_4|110\rangle \\ &\quad + y_1|111\rangle + y_2|100\rangle + y_3|010\rangle + y_4|001\rangle, \end{aligned}$$

then the symplectic structure is given by

$$\omega\big(v(x,y), v(s,t)\big) = \sum x_i t_i - \sum y_i s_i.$$

We therefore have a Poisson bracket on the polynomial functions on V given by

$$\begin{aligned} \{g,h\}\big(v(x,y)\big) = \sum \frac{\partial g}{\partial x_i}\big(v(x,y)\big)\frac{\partial h}{\partial y_i}\big(v(x,y)\big) \\ - \sum \frac{\partial g}{\partial y_i}\big(v(x,y)\big)\frac{\partial h}{\partial x_i}\big(v(x,y)\big). \end{aligned}$$

Since the action of G is symplectic it follows that the action of its Lie algebra on polynomials is given by a Poisson bracket with quadratic elements. The complexified Lie algebra of G is a direct sum of three copies of $\mathfrak{sl}(2,\mathbb{C})$. We will now write out the corresponding polynomials. Note that the Lie algebra of $\mathfrak{sl}(2,\mathbb{C})$ has basis $\{e,f,h\}$ with

$$e = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad f = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \quad h = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

So the three sets of polynomials are:

$$\begin{aligned} e_1 &= x_1x_2 - y_3y_4, \quad f_1 = x_3x_4 - y_1y_2, \\ e_2 &= x_1x_3 - y_2y_4, \quad f_2 = x_2x_4 - y_1y_3, \\ e_3 &= x_1x_4 - y_2y_3, \quad f_3 = x_2x_3 - y_1y_4, \\ h_1 &= -x_1y_1 - x_2y_2 + x_3y_3 + x_4y_4; \\ h_2 &= -x_1y_1 + x_2y_2 - x_3y_3 + x_4y_4; \\ h_3 &= -x_1y_1 + x_2y_2 + x_3y_3 - x_4y_4. \end{aligned}$$

The elements $\frac{1}{2}h_i^2 + 2e_if_i$ are all the same, and up to scalar multiple equal to the polynomial f above. One can check that $\{e_i, f\} = \{f_i, f\} = \{h_i, f\} = 0$ for $i \in \{1,2,3\}$ directly.

We now need notation for the two copies of V that come into the study of the previous section. Let $z_i = x_i$ and $z_{4+i} = y_i$ for $1 \le i \le 4$. We note that the symplectic basis used above is also orthonormal. Thus if we think of the second copy as the conjugate space using the same basis, the action of an element of K is by its conjugate and thus by the transpose inverse relative to the above basis. It is convenient to think of the z_j as $s_j + it_j$ with s_j and t_j real, and introduce new variables w_j with $w_j = -s_{j+4} + it_{j+4}$ and $w_{j+4} = s_j - it_j$ for $1 \le j \le 4$. We now note that in this context the polynomials on $V \oplus V$ (using the coordinates z_j and w_j) admit polarization operators. We set

$$D_{w,z} = \sum w_i \frac{\partial}{\partial z_i} \quad \text{and} \quad D_{z,w} = \sum z_i \frac{\partial}{\partial w_i}.$$

One checks that

$$H = [D_{w,z}, D_{z,w}] = \sum w_i \frac{\partial}{\partial w_i} - \sum z_i \frac{\partial}{\partial z_i}$$

to see that we have yet another Lie algebra isomorphic with the Lie algebra $\mathfrak{sl}(2,\mathbb{C})$ viz:

$$e \longmapsto D_{z,w}, \quad f \longmapsto D_{w,z}, \quad h \longmapsto H.$$

The action of this Lie algebra commutes with the action of K on the polynomials in the two copies of V. We now write the operators analogous to the e_i, f_i and h_i in terms of the coordinates w_i. They become:

$$\begin{aligned} E_1 &= w_1w_2 - w_7w_8, \; F_1 = w_3w_4 - w_5w_6, \\ E_2 &= w_1w_3 - w_6w_8, \; F_2 = w_2w_4 - w_5w_7, \\ E_3 &= w_1w_4 - w_6w_7, \; F_3 = w_2w_3 - w_5w_8, \\ H_1 &= -w_1w_5 - w_2w_6 + w_3w_7 + w_4w_8; \\ H_2 &= -w_1w_5 + w_2w_6 - w_3w_7 + w_4w_8; \\ H_3 &= -w_1w_5 + w_2w_6 + w_3w_7 - w_4w_8. \end{aligned}$$

We can now write down formulae for our invariants:

$$\begin{aligned} |v|^2 &= \sum z_iw_{i+4} - \sum z_{i+4}w_i \\ \psi_i &= \frac{h_iH_i}{2} + e_iF_i + f_iE_i, \quad 1 \le i \le 3 \end{aligned}$$

$$
\begin{aligned}
f &= \frac{h_i^2}{2} + 2e_i f_i \quad (\text{for any } i)\\
g = \bar{f} &= \frac{H_i^2}{2} + 2E_i F_i \quad (\text{for any } i)\\
\psi_4 &= D_{w,x} f\\
\psi_5 &= D_{z,w} g \propto D_{w,z}^3 f\\
\psi_6 &= \sum \frac{\partial f}{\partial z_i}\frac{\partial g}{\partial w_i}.
\end{aligned}
$$

Note that up to a scalar multiple

$$D_{w,z}^2 f = 2(\psi_1 + \psi_2 + \psi_3) + |v|^4.$$

The following five elements:

$$f,\ D_{w,z} f,\ D_{w,z}^2 f,\ D_{w,z}^3 f,\ D_{w,z}^4 f$$

span a representation space for the fourth action of $\mathfrak{sl}(2,\mathbb{C})$, equivalent with the 5-dimensional irreducible representation. We denote those elements by u_1, u_2, u_3, u_4, u_5. We also observe that it is well known that the algebra of invariants in the polynomials in $V \oplus V$ under the action of the four copies of $\mathfrak{sl}(2,\mathbb{C})$ is a polynomial ring in 4 generators of respective degrees $2, 4, 4, 6$. A calculation shows that an element $a_1\psi_1 + a_2\psi_2 + a_3\psi_3$ is invariant under all three actions if and only if $a_1 + a_2 + a_3 = 0$. One can check that ψ_6 is not of the form

$$|v|^2(a_1\psi_1 + a_2\psi_2 + a_3\psi_3 + a_4|v|^2)$$

for any choice of a_j, $1 \le j \le 4$. One can also show that the algebra of $\mathfrak{sl}(2,\mathbb{C})$ invariants in the polynomials on the 5-dimensional irreducible representation is a polynomial ring in two invariants, α_1 and α_2, of degrees 2 and 3.

PROPOSITION 3.5
The algebra generated by $|v|^2$, u_i $(1 \le i \le 5)$, and ψ_6 is isomorphic with the polynomial algebra in seven variables.

This result has been proved with the help of the computer algebra package Maple as follows. Form the matrix with entries

$$A_{i,j} = \frac{\partial u_i}{\partial z_j} \quad \text{and} \quad A_{i,j+8} = \frac{\partial u_i}{\partial w_j}$$

for $2 \le i \le 6$, $1 \le j \le 8$ and

$$A_{1,j} = \frac{\partial |v|^2}{\partial z_j},\ A_{1,j+8} = \frac{\partial |v|^2}{\partial w_j},\ A_{7,j} = \frac{\partial \psi_6}{\partial z_j},\ A_{7,j+8} = \frac{\partial \psi_6}{\partial w_j}.$$

Substitute "random" values for the z_i and w_i and then use Gaussian elimination to find a nonzero 7×7 minor (e.g., use C_{ij} with $i \in \{1,2,3,4,5,6,7$ and $j \in \{1,2,3,4,5,6,9\}$). Thus if $f_1 = |v|^2$, $f_{i+1} = u_i$ for $1 \le i \le 5$, and $f_7 = \psi_7$ then

$$\mathrm{d}f_1 \wedge \mathrm{d}f_2 \wedge \mathrm{d}f_3 \wedge \mathrm{d}f_4 \wedge \mathrm{d}f_5 \wedge \mathrm{d}f_6 \wedge \mathrm{d}f_7$$

is nonzero on an open dense subset of $\mathbb{C}^{16}$. This clearly implies that if h is a polynomial in 7 indeterminates and $h(f_1, f_2, f_3, f_4, f_5, f_6, f_7)$ is identically 0 then h is identically 0.

We are finally ready to give the main result on invariants:

THEOREM 3.3
The algebra of G-invariants is generated by $|v|^2, u_1, \ldots, u_5, \psi_6, \psi_1 - \psi_2$, $\psi_2 - \psi_3$.

PROOF We note that the general theory of symmetric pairs, applied to $SO(4,4)$ (a reference for this theory, used thoughout this proof, can be found in [15, Section 12.4]), implies that the algebra, I, of invariants under G annihilated by both D_{zw} and D_{wz}, is a polynomial ring in generators of degrees $2, 4, 4, 6$. We already know that the elements $|v|^2$, $\psi_1 - \psi_2$ and $\psi_2 - \psi_3$ have these additional properties. We also note that $D_{zw}(\psi_6 + \frac{|v|^2 u_3}{6}) = D_{wz}(\psi_6 + \frac{|v|^2 u_3}{6}) = 0$. Thus if we take $\alpha_1 = |v|^2$, $\alpha_2 = \psi_1 - \psi_2$, $\alpha_4 = \psi_2 - \psi_3$ and $\alpha_4 = \psi_6 + \frac{|v|^2 u_3}{6}$ then these give algebraically independent generators of the algebra I. The general theory also implies that the algebra of all polynomials on $V \oplus V$ is a free I-module under multiplication.

We also note that the same theory for the symmetric pair $(SL(3,\mathbb{R}), SO(3))$ implies that $J = \mathbb{C}[u_1, \ldots, u_5] \cap I$ is a polynomial algebra in two generators β_1 and β_2 of respective degrees 8 and 12 with

$$
\begin{aligned}
\beta_1 &= 2fD_{wz}^4 f + (D_{wz}^2 f)^2 - 2D_{wz} f D_{wz}^3 f\\
\beta_2 &= 2(D_{wz}^2 f)^3 - 6D_{wz} f D_{wz}^2 f D_{wz}^3 f + 9f(D_{wz}^3 f)^2\\
&\quad -12 f D_{wz}^2 f D_{wz}^4 f + 6(D_{wz} f)^2 D_{wz}^4 f.
\end{aligned}
$$

Furthermore, $\mathbb{C}[u_1,\dots,u_5]$ is a free J-module under multiplication and the algebra $\mathbb{C}[\alpha_1,\alpha_2,\alpha_3,\alpha_4]$ is a free $L=\mathbb{C}[\alpha_1,\beta_1,\beta_2,\alpha_4]$ module under multiplication. Thus since the algebra of all polynomials is free as a $\mathbb{C}[\alpha_1,\alpha_2,\alpha_3,\alpha_4]$-module under multiplication and the algebra $\mathbb{C}[\alpha_1,u_1,\dots,u_5,\alpha_4]$ is a module direct summand, it is thus free as an L-module under multiplication. This implies that the algebra $\mathbb{C}[\alpha_1,\alpha_2,\alpha_3,\alpha_4,u_1,u_2,u_3,u_4,u_5]$ is isomorphic with

$$\mathbb{C}[\alpha_1,u_1,\dots,u_5,\alpha_4]\bigotimes_L\mathbb{C}[\alpha_1,\alpha_2,\alpha_3,\alpha_4],$$

which has Hilbert series

$$\begin{aligned}&\frac{(1-q^8)(1-q^{12})(1-q^2)(1-q^6)}{(1-q^4)^5(1-q^2)(1-q^6)(1-q^2)(1-q^4)^2(1-q^6)}\\&=\frac{(1-q^8)(1-q^{12})}{(1-q^4)^5(1-q^2)(1-q^6)(1-q^4)^2}\\&=\frac{(1+q^4)(1+q^4+q^8)}{(1-q^2)(1-q^4)^5(1-q^6)}.\end{aligned}$$

This agrees with the Hilbert series that we calculated for the invariants in the previous section. ∎

Before we go on to the invariants for $U(2)\times U(2)\times U(2)$ a few observations about the invariants are in order. If $v\in V$ then we can construct three pairs of vectors from v. Write $v=\sum x_i|i\rangle$. Let $\alpha=(x_0,x_1,x_2,x_3)$, $\beta=(x_4,x_5,x_6,x_7)$, $\gamma=(x_0,x_1,x_4,x_5)$, $\delta=(x_2,x_3,x_6,x_7)$, $\mu=(x_0,x_2,x_4,x_6)$ and $\nu=(x_1,x_3,x_5,x_7)$. Then the pairs are (α,β), (γ,δ) and (μ,ν). In the first pair we are looking at whether or not the first (most significant) bit (of i) is 0, for the next the second bit and for the last the last bit. If u,v are vectors in $\mathbb{C}^4$ then we define $\Delta(u,v)$ to be the sum of the absolute value squared of the 2×2 minors of the matrix

$$\begin{bmatrix}u_1&u_2&u_3&u_4\\v_1&v_2&v_3&v_4\end{bmatrix}.$$

Then the invariants ψ_1, ψ_2 and ψ_3 are up to scalar multiples $\Delta(\alpha,\beta)$, $\Delta(\gamma,\delta)$ and $\Delta(\mu,\nu)$. Thus $\sum\psi_j$ is up to a scalar multiple the invariant Q defined for arbitrarily many qubits in [16].

3.6 Some implications for other representations

In this section we will show how the results in the previous sections apply to other compact Lie groups. We first observe (as in Section 3.2) that we may look upon the results as the analysis of the action of $G=SU(2)\times SU(2)\times SU(2)$ on $\mathbb{C}^2\otimes\mathbb{C}^2\otimes\mathbb{C}^2\otimes\mathbb{C}^2$ via $g\otimes I$. The group $U(2)$ acting only on the last factor commutes with the action of G. We will now rewrite the formula in Proposition 3.3 to take into account the total homogeneity. In other words we write $q=qx$ and $t=qx^{-1}$. The formula now becomes

$$\frac{(1+q^4)(1+q^4+q^8)}{(1-q^2)(1-q^4x^4)(1-q^4x^2)(1-q^4)(1-q^4x^{-2})(1-q^4x^{-4})(1-q^6)}.$$

We note that the variable x can be thought of as the parameter of the circle subgroup, T, of all

$$\begin{bmatrix}x&0\\0&x^{-1}\end{bmatrix}$$

in the $SU(2)$ acting on the fourth variable, and the formula above is just the q-character for the action on the G-invariants. In [17] the q-multiplicity formulae for the action of $SU(2)$ on the spin-2 (5-dimensional) representation was determined. Set $W=F^2$. Then $m_{F^2}(q,k)=0$ if k is not an integer. If $k=2l$ is an even integer we have

$$(1-q^2)(1-q^3)m_W(q,2l)=q^l+q^{l+1}+\dots+q^{2l}=q^l\frac{1-q^{l+1}}{1-q}.$$

If $k=2l+3$ then we have

$$m_W(q,2l+3)=q^3m_W(q,2l).$$

One can prove this by observing that these formulae satisfy

$$\begin{aligned}&\frac{1}{(1-qx^4)(1-qx^2)(1-q)(1-qx^{-2})(1-qx^{-4})}\\&=\sum_{k\geq 0}m_W(q,k)\frac{x^{2k+1}-x^{-2k-1}}{x-x^{-1}}.\end{aligned}$$

We first note that this gives an alternate proof of Proposition 3.3 since that proposition describes the Hilbert series of the invariants for the

action of T on the polynomial invariants. Note that there is a shift $q \to q^4$. Thus since every repesentation F^k with k an integer has a T-fixed vector, we see that the Hilbert series for the action of $S^1 \times G$ as in Section 3.3 is

$$\frac{(1+q^4)(1+q^4+q^8)}{(1-q^2)(1-q^6)} \sum_{k\geq 0} m_W(q^4,k).$$

We leave it to the reader to check that this formula agrees with Proposition 3.3. We also note that, on the other hand, Proposition 3.3 can be used to derive information about the series $m_W(q,k)$.

More seriously, we note that our formulae give information about 4 qubits:

COROLLARY 3.2
Let $SU(2) \times SU(2) \times SU(2) \times SU(2)$ act on $U = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ as above. Then

$$m_U\big(q,(0,0,0,k)\big) = \frac{(1+q^4)(1+q^4+q^8)}{(1-q^2)(1-q^6)} m_{F^2}(q^4,k).$$

References

[1] M. H. Freedman, Poly-locality in quantum computing, quant-ph/0001077.

[2] P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in S. Goldwasser, Ed., *Proceedings of the 35th Symposium on Foundations of Computer Science*, Santa Fe, NM, 20–22 November 1994 (Los Alamitos, CA: IEEE Computer Society Press 1994) 124–134;
P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM J. Comp.* **26** (1997) 1484–1509.

[3] D. Coppersmith, An approximate Fourier transform useful in quantum factoring, *IBM Research Report RC 19642* (12 July 1994).

[4] A. Einstein, B. Podolsky and N. Rosen, Can quantum-mechanical description of physical reality be considered complete?, *Phys. Rev.* **47** (1935) 777–780.

[5] D. Bohm, *Quantum Theory* (New York: Prentice-Hall 1951).

[6] J. S. Bell, On the Einstein-Podolsky-Rosen paradox, *Physics* **1** (1964) 195–200.

[7] E. Schrödinger, Die gegenwärtige Situation in der Quantenmechanik, *Naturwissenschaften* **23** (1935) 807–812; 823–828; 844–849.

[8] E. M. Rains, Polynomial invariants of quantum codes, *IEEE Trans. Inform. Theory* **46** (2000) 54–59.

[9] N. Linden and S. Popescu, On multi-particle entanglement, *Fortsch. Phys.* **46** (1998) 567–578.

[10] M. Grassl, M. Rötteler and T. Beth, Computing local invariants of quantum-bit systems, *Phys. Rev. A* **58** (1998) 1833–1839.

[11] A. Sudbery, On local invariants of pure three-qubit states, *J. Phys. A: Math. Gen.* **34** (2001) 643–652.

[12] J.-L. Brylinski and R. Brylinski, Invariant polynomial functions on k qudits, quant-ph/0010101. In Chapter 11 of this book.

[13] M. Grassl, Description of multi-particle entanglement through polynomial invariants, talk presented at the *Workshop on Complexity, Computation and the Physics of Information*, Isaac Newton Institute for Mathematical Sciences, Cambridge, UK, 22 July 1999;
http://iaks-www.ira.uka.de/home/grassl/paper/CCP.ps.gz.

[14] B. Gross and N. Wallach, On quaternionic discrete series representations, and their continuations, *J. Reine Angew. Math.* **481** (1996) 73–123.

[15] R. Goodman and N. Wallach, *Representations and Invariants of the Classical Groups, Encyclopedia of Mathematics and its Applications* **68** (Cambridge, UK: Cambridge University Press 1998).

[16] D. A. Meyer and N. Wallach, Global entanglement in multiparticle systems, quant-ph/0108104.

[17] N. Wallach and J. Willenbring, On some q-analogs of a theorem of Kostant-Rallis, *Canad. J. Math.* 52 (2000) 438–448.